

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

United States Courts
Southern District of Texas
FILED

MAR 19 2018

David J. Bradley, Clerk of Court

United States of America

v.

Tokishia Monique Bruno

Case No.

H18-0384M

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of N/A in the county of Harris in the
Southern District of Texas, the defendant(s) violated:

Code Section

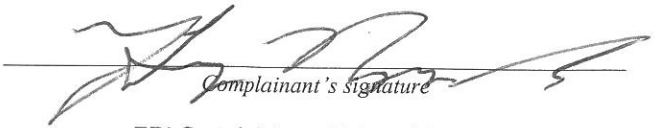
18 U.S.C. §1349 (conspiracy to
commit wire fraud)

Offense Description

In or about December 2016, within the Southern District of Texas, the
 defendant, Ndubuisi Nwandu and Tokishia Monique Bruno, did knowingly
 combine, conspire, confederate and agree with each other and others known
 and unknown, to commit the following offense against the United States: wire
 fraud, in violation of 18 USC 1343, all in violation of 18 USC 1349.

This criminal complaint is based on these facts:

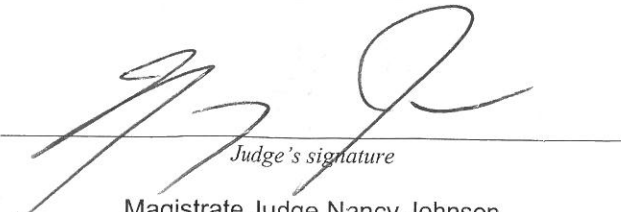
Please see attached affidavit.

☒ Continued on the attached sheet.


FBI Special Agent Hong Nguyen

Printed name and title

Sworn to before me and signed in my presence.

Date: 3-19-18City and state: Houston, Texas


Magistrate Judge Nancy Johnson

Printed name and title

H18-0384M

AFFIDAVITUnited States Courts
Southern District of Texas
FILED

I, Special Agent Hong Nguyen, Jr., being first duly sworn, hereby depose and state, as follows:

MAR 19 2018

Summary

David J. Bradley, Clerk of Court

The FBI is investigating a conspiracy to steal money from corporate victims through business email compromises. Essentially, conspirators will pose as business partners (e.g. suppliers) of these corporate victims, and send an email asking that payments be routed to a “new” account belonging to the “business partner.” When the corporate victim sends the money, the conspirators will withdraw the money as soon as it becomes available – and before the victim can realize its mistake and cancel the transaction. The conspirators continue to be engaged in this and similar frauds as recently as at least January 2018. Thus, the FBI seeks warrants to arrest two of these conspirators: Ndubuisi Nwandu and Tokishia Bruno.

Introduction and Agent Background

1. I make this affidavit in support of criminal complaint filed against an application for a warrant to arrest the people listed below for violations of 18 U.S.C. §§ 1349 (conspiracy to commit wire fraud):

(1) Ndubuisi George Nwandu, DOB 9/21/1988

(2) Tokishia Monique Bruno, DOB 9/22/1978

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and assigned to a Cyber Crimes Task Force in the Houston, Texas division. I have been employed as a Special Agent with the FBI since May 2016. As a Special Agent of the FBI, I am charged with the duty of investigating violations of the laws of the United States, collecting evidence in cases in which the United States is or may be a party in interest, and performing other duties imposed by law. I investigate crimes involving the unauthorized intrusion into a computer or network such as computer intrusions, business email compromises, distributed denial-of-service attacks, and financially motivated attacks.

3. Prior to this assignment, I was assigned as a Digital Forensic Examiner at the FBI Greater Houston Regional Computer Forensics Laboratory since 2013 where I worked a variety of matters, many of which included a significant cyber component. I have training in the preparation, presentation, and service of criminal arrest and search warrants, and have been involved in the investigation of offenses against the United States, including fraud and related activity in connection with computers. I also have a Bachelor of Science degree in Computer Information Systems and a Master of Business Administration with a Post Graduate Certificate in Information Assurance. References to my training and experience also incorporate the training and experience of FBI Special Agent Jeffrey Anderson.

4. The facts set forth in this affidavit are based upon my own personal observations, my training and experience, as well as information obtained during this investigation from other sources, including: (a) other agents from the FBI, and other law enforcement personnel involved

in this investigation; (b) statements made or reported by various witnesses with personal knowledge of relevant facts; and (c) my review of records obtained during the course of this investigation, as well as summaries and analyses of such documents and records that have been prepared by others.

5. Because this affidavit is submitted for the limited purpose of obtaining a search warrant, I have not set forth each and every fact I have learned in connection with this investigation. Conversations and events are related in substance and in part.

Facts Supporting Probable Cause

Business email compromises, generally

6. The FBI is investigating a business email compromise scheme that targets corporate victims. Essentially, the conspirators pose as business partners (such as suppliers) of these corporate victims, and send fraudulent emails, saying that the "supplier" has changed banks, and asks that payments be sent to a new bank account (an account actually controlled by the conspirators). The corporate victims think they are paying their suppliers, but in reality, their suppliers have no idea these emails are being sent, and the corporate victims are being defrauded. Once the corporate victims send the money, the conspirators withdraw the money before it can be frozen.

After receiving an invoice purporting to come from one of its suppliers, victim Steel Surplus pays \$48,018.00 to Capital One bank account 5610

9. For example, around December 9, 2016, victim Steel Surplus was defrauded when someone spoofed (impersonated) the email address of one of Steel Surplus' suppliers, Cumic Steel. Previously, the victim ordered steel beams from Cumic Steel, communicating with David Cui at Cumic Steel via his email address dcui@cumicusa.com.

10. Around December 9, 2016, the ^{CEO of the} victim received ^{in Houston, TX} an email purporting to come from David Cui. Like prior emails, this email displayed David Cui's name. It also seemed to reply to prior legitimate correspondence between the parties as they negotiated their deal. Even reviewing the "from" line in the email's header information, I saw that the email displayed David Cui's correct email address: dcui@cumicusa.com.

11. However, when I viewed the header information on this email, I saw that if the victim replied to this email, replies would actually be directed to "dcui@curmicusa.com."

From: "David Cui" <dcui@cumicusa.com>
 Subject: Re: Beams
 To: usfencehouston@aol.com
 Content-Type: multipart/mixed; boundary="ki2mtweG8GBB8RsLmE7yZyoKh3L=_9Cr670"
 MIME-Version: 1.0
 Reply-To: dcui@cumicusa.com
 Date: Sat, 10 Dec 2016 00:24:10 -0100
 X-Antivirus: avast! (VPS 160622-1, 06/22/2016). Outbound message

12. This fraudulent email purported to update the victim on the status of the victim's order – and also instructed the victim to wire payment to Capital One Bank, account number 5610 (all references to bank accounts here only list the last four digits), referencing the account name, "Valyn Consulting."

13. On or around December 13, 2016, the victim complied and wired \$48,018.00 to Capital One bank account 5610.

14. Later, Cumic informed the victim Steel Surplus that the wire was never received. Ultimately, the order was not fulfilled by Cumic Steel. Victim Steel Surplus lost the \$48,018.00.

The signatory for Capital One bank account 5610 is Tokishia Bruno

15. Capital One's records show that \$48,018.00 was wired from Steel Surplus, Inc. into Capital One account 5610 on December 14, 2016 (a \$15.00 wiring fee was also incurred).

16. These records identified the owner of this as being Tokishia M Bruno doing business as (d/b/a) Valyn Consulting. This account was opened with Tokishia Bruno's social security number and Texas driver's license number.

As soon as the \$48,018.00 transfer from Steel Surplus cleared, Bruno ordered several cashier's checks made out to Ndubuisi Nwandu before the transaction could be rescinded

17. The same day that the \$48,018.00 from Steel Surplus was available, Bruno withdrew a total of \$38,720.60 before the transaction could be rescinded. The following day, she withdrew another \$4,500.

18. The bank teller's ledger revealed that \$38,720.60 withdrawal on December 14, 2016, took the form of five (5) cashier's checks in the amounts of:

- \$8,587.16 paid to Ndubuisi Nwandu
- \$6,280 paid to Ndubuisi Nwandu
- \$11,040.98 paid to Tokishia Bruno Univ of North Texas
- \$5,500 paid to Tokishia Bruno
- \$7,312.46 paid to Your Journey Girl Travel Services (Bruno)¹

19. Bruno's participation is corroborated by the Capital One's security cameras which recorded Bruno around the same time and date as these transactions. For example, Capital One's

¹ Emails suggest that "Your Journey Girl Travel Services" is a travel service operated by Bruno. For example, on Dec. 2, 2016, "Journey Girl <YJG4Travel@gmail.com>" emailed flight confirmation for both Bruno and Nwandu to Nwandu's gmail account (NduNwandu@gmail.com). In turn, this email listed Bruno's email address as "YJG4Travel@gmail.com," which I understand to reference Your Journey Girl for Travel.

security camera footage showed that on December 14, 2016, someone consistent with Bruno's appearance approached a Capital One bank teller at its Carrollton branch. This corresponds with Bruno's December 2016 Capital One statement, which listed only one transaction that occurred on that date and which also required an in-person visit: the \$38,720.60 customer withdrawal.

20. The fact that it was Bruno is further corroborated by the fact that a Capital One fraud investigator contacted Bruno. In a voice recording provided by Capital One, a fraud investigator contacted Bruno around January 6, 2017, and Bruno stated the money was received from an organization named ORCA, a science technology and math (STEM) program for girls, who requested her to organize an event, book airline tickets, and vendors for a group of girls traveling from Cameroon and South America (i.e. Argentina) to the United States – all of which is contradicted by the fact that the money (a) did not come from ORCA, and (b) mostly went to Nwandu and Bruno.

21. Moreover, Bruno admitted that she still had approximately \$5,500 of the money and promised to return it to Capital One. However, on February 14, 2018 – more than a year later – Capital One reported that Bruno never returned the funds.

22. Bruno also gave cashier's checks to Nwandu on other occasions. For example, records from Bruno's Capital One account showed a cashier's check paid to Ndubuisi Nwandu: October 6, 2016, in the amount of \$4,000.00.

Tokishia Bruno was also one of the people who received proceeds from another business email compromise involving victim EMR

23. According to Rosie Shako, an Operations Manager employed at Enviro Management and Research, Inc. (EMR), EMR was also the victim of fraudulent activity. Around August 2016, Shako received a legitimate email from Employee 1, a Project Manager in EMR's Myanmar division. This email attached an invoice for \$18,587.50, and asked her to wire funds to Chua Eu International PTE LTD ("Chua"), a vendor located in Singapore.

24. Later, Shako received a fraudulent email purporting to be from Employee 1, again asking her to pay vendor Chua, but instead, asking her to wire funds to Wells Fargo Bank account 4763. Shako complied – but EMR was later notified by the vendor, Chua, that Chua never received payment. EMR learned that Employee 1's laptop computer had been hacked, and that the attacker was able to use a template to send a wire request that appeared authentic.

25. The FBI obtained records from Wells Fargo for account number 4763, which revealed that on August 17, 2016, EMR's \$18,587.50 was sent to a Wells Fargo Bank account. That account was in the name of "K&K Oil Service" in Round Rock, TX, held by Kathleen Calarco. Calarco withdrew \$18,500 from her Wells Fargo account on August 18, 2016.

26. First, on August 18, 2016, Tokisha Bruno deposited \$9,000 to Capital One account 5610. This was Tokishia Bruno's Capital One 5610 account that had been used to defraud Steel Surplus, as described above.

Nwandu also participated in another fraud scheme

27. Around June 30, 2017, a victim reported that she had sought funding for an online business that she wanted to start, and spoke to a friend whom she met online – but whom she had never met – named Dan Henderson.

28. She received an envelope to their home address with a “funding” check inside from a victim company for approximately \$34,545.69. As instructed by Dan Henderson, around July 3, 2017, the victim obtained two \$9,000 cashier’s checks (total \$18,000) to Trevion Trice, 1846 E. Rosemeade Pkwy, #146, Carrollton, TX 75007-2637. On or around July 5, 2017, the victim mailed two more cashier checks for \$9,000 and \$5,000 to the same address, respectively, to Chukwuma Okoye, an associate of Nwandu. Previously, around May 2017, Henderson requested the victim to send cashier checks to Cookie Arestida in the amount of \$8,500 and John Waithuki in the amount of \$8,000, an associate of Nwandu. Altogether, the victim mailed approximately \$49,500 to that address.

29. On or about July 6, 2017, the victim was notified via email and phone from their bank that the “funding” check that the victim received had actually been forged, and that the bank deducted the money from the victim’s account. The victim called her local police.

30. Investigator Duzan from Chaska Police Department obtained a copy of the cashier’s checks that the victim ordered to Trevion Trice, and provided these checks to the FBI. He also googled the address, he learned that 1846 E. Rosemeade Pkwy, #146, Carrollton, TX was actually a post office box at Ship N More. The owner of Ship N More told the officer that he had long suspected the renter of Box 146 to be engaged in fraud; for example, one week, Box 146 received a large number of letters, most of which appeared to be rejection letters for credit cards. Much mail to that box was also addressed to a number of other people. Further, each time the renter came to collect from his box, he parked at the far end of the strip mall, and came inside alone, apparently for the purpose of making it more difficult to identify his vehicle. The owner of Ship N More identified the renter as a black male with a thick accent that he believed was African, and noted that the renter always paid his rental fees in cash.

31. Paperwork for the renter of Box 146 showed that he had provided a New York driver’s license. I submitted a request to have the New York driver’s license number run through our internal databases and there were no results found, which suggests to me that this was a fake driver’s license.

32. I provided the owner three pictures and asked him if any of these pictures showed “Larry Thompson.” The owner identified the photo depicting Ndubuisi Nwandu.

33. Separately, around September 20, 2016, Carrollton Police Department officer Lauryl Duncan worked with a surveillance team to identify the renter of Box 146. They followed him after he picked up mail from Box 146 and, when the renter was observed failing to signal during a lane change, he was stopped by police. Police saw that his driver’s license listed his name: Ndubuisi George Nwandu.

As of January 2018, Nwandu is still participating in business email compromise frauds

34. In January 2018, the Garland High School 2018 Senior Class Booster Club also became a victim of this business email compromise. Garland Police Department reported that the treasurer of the booster club received a fraudulent email appearing to come from the club's president. At this email's direction, around January 4, 2018, the treasurer issued a \$3,200 check payable to BMW Tradings, and mailed it to 4009 Old Denton Rd #114265, Carrollton, TX 75007.

35. According to bank records obtained by police, the check was deposited around January 05, 2018 into Capital One, N.A. account 9676, an account opened by Margaret Munyenye d/b/a BMW Tradings the previous month (Dec. 7, 2017). A few days later (unlike a wire transfer, a check probably needed a few days to clear), \$2000 and \$1000 were withdrawn before the booster club could freeze the money.

36. Nwandu and his co-conspirators are connected to this transaction by the address to which the booster club mailed the check: 4009 Old Denton Rd #114265. This address is a mailbox operated by a postal center called The Carrollton Mailroom. First, an employee at The Carrollton Mailroom identified a picture of Nwandu as being someone who frequently checks this mailbox.

37. Second, this employee also sent to the FBI a picture of the person he identified as someone who frequently checks the mailbox (Nwandu) walking to a white Lexus SUV.

38. Third, this is also consistent with the fact that Carrollton Police Department records show that around August 29, 2017, a Carrollton PD officer performed a traffic stop on a white Lexus with Texas license plate 78H8754, and the driver produced a driver's license confirming that his name was Ndubuisi Nwandu. (Although those Carrollton PD records did not list the type of vehicle, later FBI surveillance around September 12, 2017 (as described below) observed Nwandu driving a white Lexus RX350 SUV, with the same temporary license plate.)

Nwandu and Bruno also continue to be engaged in marriage fraud

45. In addition, messages from Nwandu's email account also show that he and Bruno engaged in marriage fraud in violation of 8 U.S.C. § 1325(c).

46. Nwandu used NduNwandu@gmail.com. For example, Android phones prompt their users to link the phone with a Gmail account. The phone that CBP examined when Nwandu entered the country (a Samsung SM-G935T Galaxy S7 Edge, serial number (s/n) RF8HA28CR7T, International Mobile Equipment Identity (IMEI) 35852107084485) was linked with NduNwandu@gmail.com. As part of this investigation, the FBI obtained a warrant to search this email account. The earliest emails in this account are dated December 4, 2015; Keshia Bruno's earliest email is dated December 17, 2015.

47. According to Bruno's I-130 Petition for Alien Relative, Nwandu was a Nigerian citizen who, after marrying Bruno, was approved to become a conditional permanent resident alien on November 8, 2016.

48. However, on October 10, 2016, a few weeks before Nwandu's citizenship interview with USCIS was scheduled, Bruno emailed Nwandu their "Nuptial Agreement" which helpfully described the terms of their fraudulent marriage.² In this agreement, "Ndu" (defined as "Ndubuisi Nwandu") agreed to pay "Keshia" (defined as "Tokishia Bruno") (1) \$10,000 before his initial interview to acquire a conditional permanent resident card, and (2) another \$10,000 filing a petition to remove the conditional status of the permanent resident card.

7. Payments. Ndu agrees to remit payment to Keshia in the sum of \$10,000 prior to the initial interview to acquire that conditional permanent resident card. Should the conditional permanent resident card not be awarded, Keshia agrees to refund payment to Ndu or to pursue other channels toward acquirement of the conditional permanent resident at Ndu's discretion. Ndu agrees to remit payment to Keshia of \$10,000 upon filing of Form I-751 Petition to Remove the Conditions of your Green Card to be submitted 90days or less before expiration of the conditional permanent resident card. Anticipated date is in 2018.

49. This agreement voided their previous verbal agreements "(i.e. purchase of BMW vehicle, tuition discount, etc)."

12. Previous Agreements. Each party agrees that any previous verbal agreements not listed in this written nuptial agreement is void. (i.e. purchase of BMW vehicle, tuition discount, etc)

50. Nwandu and Bruno's agreement also anticipated that this agreement would expire once Nwandu acquired unconditional green card status:

3. Expiration. The provisions of this Agreement will expire upon Ndu's acquirement of permanent resident card without conditions i.e. 10-year permanent residence status. Anticipated date in 2018.

51. Nwandu and Bruno agreed to divorce once Nwandu acquired his green card:

5. Divorce or Legal Separation. Each party agrees to remain legally married throughout the duration of the process to acquire permanent residence without conditions. The marriage agreement includes income taxes to be filed married filing jointly and other joint assets such as lease agreements, bank accounts, etc as required. Each party agrees to legally divorce (uncontested) upon Ndu's acquirement of his permanent resident card without conditions. Ndu agrees to assume full financial responsibility for payment of divorce.

² On August 1, 2016, a few months before Bruno emailed this "Nuptial Agreement" to Nwandu, court records show that Bruno filed a petition for divorce. After Bruno emailed this "Nuptial Agreement," however, this agreement apparently memorialized the new understanding between Bruno and Nwandu, and Bruno abandoned her divorce petition as court records show that it was later dismissed for want of prosecution.

52. In fact, they also agreed to not have children with anyone else until their agreement expired in order “to not complicate the divorce process.” (They also agreed that sexual activity was not required or even expected.)

10. Intimacy. Each party acknowledges that physical and/or sexual activity is not a requirement or expectation of this agreement. *Each party agrees NOT to give birth with any potential/current/future suitor until the expiration of this contract as to not complicate the divorce process.*

Bruno also sent Nwandu editable bank statements, pay stubs, and other documents that are often used as fraudulent means to prove non-existent work history and income

53. On September 15, 2016, Bruno emailed Nwandu an MS Word template for fake pay stubs – documents that based on my training and experience, I know can be used to substantiate work history or income. Bruno’s email also warned Nwandu to be “careful with formatting and calculations.”

CO. FILE DEPT. CLOCK VCHR. NO. 1
VSG 561758 118100 640 0000155207 052-0035

AMAZON.COM KYDC LLC
P.O. BOX 80726
SEATTLE, WA 98108

Earnings Statement

Period Beginning: 04/03/2016
Period Ending: 04/09/2016
Pay Date: 04/15/2016

Taxable Marital Status: Single
Exemptions/Allowances:
Federal: 1
TX: No State Income Tax

FIRST NAME LAST NAME
0000 STREET NAME
DALLAS, TX 75243

Earnings rate	hours	this period	year to date	Important Notes
Regular	15.50	40.00	\$726.86	
GROSS PAY		\$520.00	\$7726.86	
Deductions		Statutory		
Federal Income Tax		\$65.91	\$818.52	
Social Security Tax		\$38.44	\$482.66	
Medicare Tax		\$8.59	\$111.29	
NET PAY		\$506.66	\$8135.12	
Checking Dep.				
NET CHECK		\$506.66	\$8135.12	

Your federal taxable wages this period are \$620.00

AMAZON.COM KYDC LLC
P.O. BOX 80726
SEATTLE, WA 98108

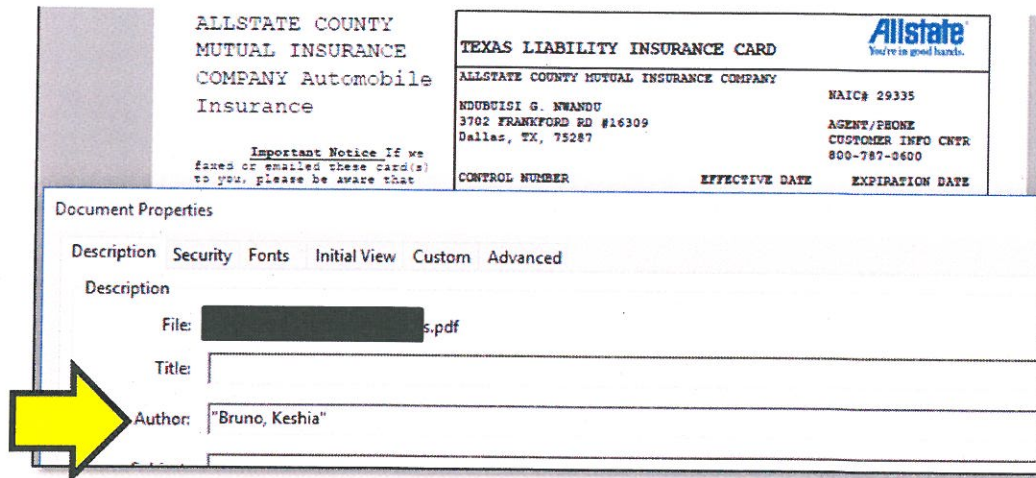
Advice number: 0000155207
Pay date: 04/15/2016

Deposited to the account of FIRST NAME LAST NAME
account number XXXXXXXXXXXX9301
transit XXXX
ABA XXXX
amount \$506.66

NON-NEGOTIABLE

54. On March 1, 2017, Bruno again emailed Nwandu, saying that she had sent him a “word doc that you can edit.” She attached an MS Word template for fake Capital One bank statements.

55. On other occasions, Bruno sent Nwandu .PDFs of various documents – but when I viewed the properties of these .PDFs, I saw that the author was actually “Bruno, Keshia.” For example, on November 22, 2016 and February 15, 2017, Bruno emailed Nwandu fake proofs of insurance.



56. Similarly, on October 9, 2016, Bruno also emailed Nwandu a fake pay stub in the name of another person that purported to document work history and income from Southwest Airlines. (Again, the properties of this .PDF listed the author as “Bruno, Keshia.”)

TECHNICAL TERMS

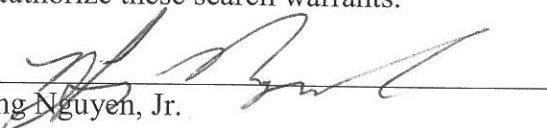
70. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.
- b. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.
- c. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- d. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g.,

121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

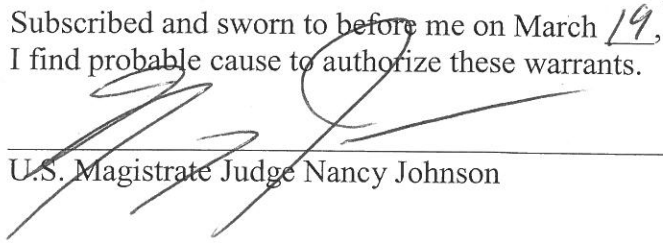
- e. “Records” and “information” include all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

71. For these reasons, I ask the Court to authorize these search warrants.



Hong Nguyen, Jr.
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on March 19th, 2018.
I find probable cause to authorize these warrants.



U.S. Magistrate Judge Nancy Johnson